Defense Information Systems Agency

A Combat Support Agency

Computing Service Directorate

Information Assurance Process

Patrice Wilmot
CSD Chief of Staff (CSS)

20 April 2009

DISA

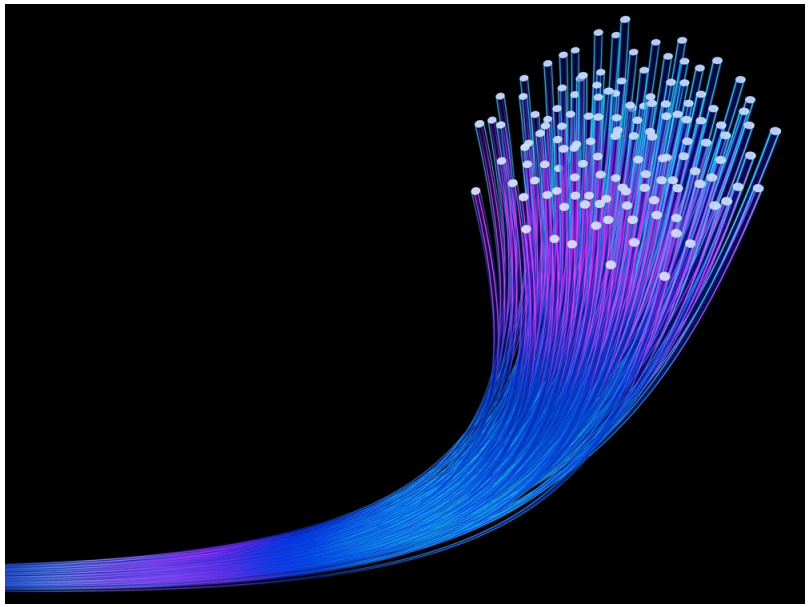
A Combat Support Agency

Securing our Infrastructure "One Security"

DISA
A Combat Support Agency

Discussion Points

- Background
- Process
- Controls
- Access
- Initiatives



DISA
A Combat Support Agency

Background

- **Challenge**
  - **Standardize IA across Computing Services**
  - **Improve customer support**

- **Process Improvement**
  - **Organizational restructure**
  - **Review of all processes**
  - **Standardization across organization**
  - **Streamline end-to-end process**

DISA
A Combat Support Agency

IA Process

- **Requirements to enter DECC**
  - **Active ATO/IATO/IATT**
    - **Certifier's Recommendation**
    - **Residual Risk Assessment**
  - **DIACAP**
    - **Executive Package**
      - **System Implementation Plan (SIP)**
      - **DIACAP Implementation Plan (DIP)**
      - **DIACAP Scorecard (EMASS scorecard is acceptable)**
      - **Approved IT POA&M**
    - **All Ports, Protocols and Services registered**
      - **Unevaluated ports mitigated**
    - **Vulnerability Compliance Assessment and Reports**
      - **STIG and IAVM**
      - **Application Security Checklist**

90 Days

DISA
A Combat Support Agency

IA Control Definitions

- **Inherited *(34)***
  - **Control that is the sole responsibility of the enclave**
    - **Continuity (3)**
    - **Security Design and Configuration (2)**
    - **Enclave and Boundary Defense (5)**
    - **Enclave and Computing Environment (3)**
    - **Physical and Environmental (21)**
- **Program/System-Owned *(28)***
  - **Control that is the sole responsibility of the program/system**
- **Negotiable *(95)***
  - **Control where an agreement must be established**
  - **Control shared between enclave and**

DISA
A Combat Support Agency

A Control Examples

Control Number	Control Name	Description	CCC	DECC	Program/System
EBPW-1 (Inherited)	Public WAN Connection	Connections between DoD enclaves and the Internet or other public or commercial wide area networks require a DMZ.	Connection of enclaves and the internet or other public or commercial WANs is the responsibilities of the CCC. OPR: CD4 & CD2	Inherited – From CCC	Inherited – From CCC
COAS-1 (Negotiable)	Alternate Site Designation	An alternate site is identified that permits the partial restoration of mission or business essential functions.	CSD has network support redundancy between the two physical Consolidated Communication Centers.	CSD has designated alternate COOP sites. This information is available from the CSD BCP Coordinator. An exemption to this would be customer who designates another entity as their alternate site. CSD designates COOP personnel to solicit, develop and maintain COOP documentation.	Must identify the requirement in the SLA for COOP, as well as whether or not they require a solution other than a designated CSD site. Must identify the requirements, as outlined in the CSD Catalog of Services, and document in the SLA. Must provide a functional COOP Plan for their application.
DCCT-1 (Program/System -Owned)	Compliance Testing	A comprehensive set of procedures is implemented that tests all patches, upgrades, and new AIS application prior to deployment.	N/A - CCC The CCC complies with the CSD Change Management Plan and coordinates changes with the applicable DECCs.	N/A - DECCs The DECCs do not perform functionality testing. They do comply with the CSD Change Management Plan and coordinates changes through the customer.	The customer is responsible for any functionality/compatibility testing for system changes/security patches and provides authorization to the DECC for implementation. If the customer cannot comply with a specified requirement, in relation to a JTF Directive or STIG, they must provide a detailed POA&M explaining the get well plan.

DISA
A Combat Support Agency

IA Process

DITSCAP → DIACAP

ON CYBER PATROL
As covered or mandated by AR 25-2
THE NEW CERTIFICATION AND ACCREDITATION PACKAGES ARE IN, AND THEY'RE ALL ON THE TRUCK. I NEED YOUR HELP GETTING THEM OFF.
LAST YEAR, IT TOOK US ALL DAY TO UNLOAD THEM.
DITSCAP
EST. 1997
BUT SARGE, THEY'VE CHANGED--
I DON'T CARE. COME HELP ME.
WHICH END DO YOU WANT ME TO CARRY?
DIACAP
EST. 2007
A025

DISA
A Combat Support Agency

Privileged Access

Definition:

"An authorized user who has access to system control, monitoring, administration, criminal investigation, or compliance functions."

Customer will determine the level of user privilege for that database. In no case, will it be less than IT-II level. These users will be "Privileged."

All remote and local access for "Privileged" users will employ security measures that encrypt the transmission from workstations to source server with FIPS 140-2 compliant encryption (i.e., OOB, VPN, SSL, etc.)

Use of "Privileged" accounts should be limited to privileged functions

DISA
A Combat Support Agency

OOB Access

- **Requires OOB**
  - **Privileged access SUDO/Root**
    - **Administrator**
    - **Server configuration changes**
      - ***Complete list in Application Services and Web Server STIG***

- **Does <u>Not</u> require OOB**
  - **Non-privileged activities (examples):**
    - **Create/Delete non-privileged accounts**
    - **Reset passwords**
    - **File Uploads and Downloads**
    - **Web content management specific to roles**
    - **Start/Stop Specific Services**

** ***Root access limited to CSD personnel***

DISA
A Combat Support Agency

Initiatives

- **We are Securing our Infrastructure**
  - ✓ **Developing:**
    - **Continuous process improvement**
    - **Test and Development environment**
  - ✓ **Implementing:**
    - **HBSS {CTO 07-12}**
    - **DOD Whitelist {CTO 08-01}**
  - ✓ **Changing:**
    - **Operational tempo**
    - **Personal Identifiable Information (PII)**

DISA

A Combat Support Agency

Securing our Infrastructure

“One Security”
Shared Responsibility
Shared Risk

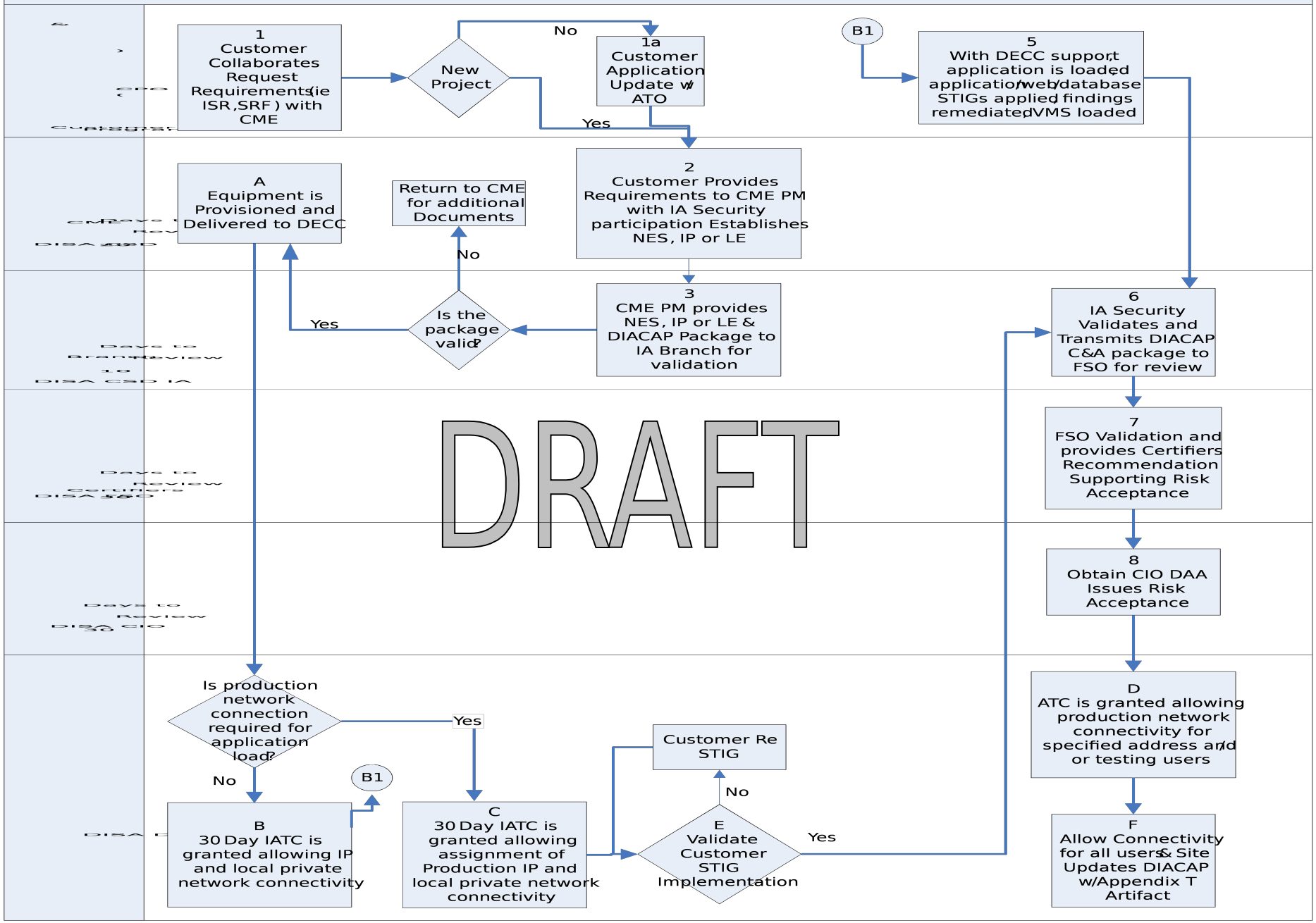
www.disa.mil

DISA
A Combat Support Agency

Definitions

- **Interim Authorization to Test (IATT)**
  - **Temporary authorization to test information system**
    - **Operational environment necessary**
    - **Live data necessary**
    - **Specified time period**
- **Interim Authority to Operate (IATO)**
  - **Temporary authorization to operate information system**
- **Authority to Operate (ATO)**
  - **Authorization to operate information system**
    - **All assigned IA controls implemented to ensure acceptable residual risk**
    - **May be assigned for up to 3 years, reviewed annually**

Information System IA Implementation Process


1
Customer Collaborates Request Requirements(ie ISR,SRF) with CME
New Project
No
1a
Customer Application Update w/ ATO
Yes
2
Customer Provides Requirements to CME PM with IA Security participation Establishes NES, IP or LE
3
CME PM provides NES, IP or LE & DIACAP Package to IA Branch for validation
Is the package valid?
No
Return to CME for additional Documents
Yes
A
Equipment is Provisioned and Delivered to DECC
B1
5
With DECC support, application is loaded, application/web/database STIGs applied, findings remediated, VMS loaded
6
IA Security Validates and Transmits DIACAP C&A package to FSO for review
7
FSO Validation and provides Certifiers Recommendation Supporting Risk Acceptance
8
Obtain CIO DAA Issues Risk Acceptance
D
ATC is granted allowing production network connectivity for specified address and/or testing users
F
Allow Connectivity for all users & Site Updates DIACAP w/Appendix T Artifact
Is production network connection required for application load?
Yes
No
B
30 Day IATC is granted allowing IP and local private network connectivity
B1
C
30 Day IATC is granted allowing assignment of Production IP and local private network connectivity
Customer Re STIG
No
E
Validate Customer STIG Implementation
Yes
DRAFT